REMARKS

The Office Action mailed September 4, 2008 has been carefully considered. Reconsideration in view of the following remarks is respectfully requested.

Claim Status and Amendment of the Claims

Claims 1-2, 5-12, 15-21, and 24-41 are currently pending.

No claims stand allowed.

Claims 3-4, 13-14, and 22-23 were previously cancelled without prejudice or disclaimer of the subject matter contained therein.

Claim 21 has been amended to further particularly point out and distinctly claim subject matter regarded as the invention. Support for these changes is found in the specification, figures, and claims as originally filed.

The 35 U.S.C. § 102 Rejection

Claims 1-10, 30-35, and 40-41 stand rejected under 35 U.S.C. § 102 as allegedly being anticipated by Meier et al.,[1] among which claims 1, 30, and 40-41 are independent claims.[2] [3] This rejection is respectfully traversed.

Claims 3-4 were previously cancelled without prejudice or disclaimer of the subject matter contained therein, rendering the rejection moot as to Claims 3-4.

[1] U.S. Publication No. 2005/01856 to Meier et al.

[2] Office Action mailed September 4, 2008, at p. 3.

[3] Office Action at p. 3.

Improper Omnibus Rejection

As an initial matter, the Applicant submits that the omnibus rejection of Claims 1-10, 30-35, and 40-41 under 35 U.S.C. § 102 is improper. The M.P.E.P. states:

> A plurality of claims should never be grouped together in a common rejection, unless that rejection is equally applicable to all claims in the group.[4]

The Examiner has grouped 6 independent claims into a single omnibus rejection under 35 U.S.C. § 102. The rejection refers to the term "determining if said user device supports a user authentication protocol." Claims 1, 30, and 31 refer to refer to "determining if said user device supports a user authentication protocol," while Claims 32, 40, and 41 refer to "allowing the user device limited access to a network via the network access device *if it is determined that the user device is unable to communicate using a particular user authentication protocol*." (emphasis added) The omnibus rejection under 35 U.S.C. § 102 is therefore not equally applicable to all claims in the group and is thus improper.

Turning to the substance of the rejection, according to the M.P.E.P., a claim is anticipated under 35 U.S.C. § 102(a), (b) and (e) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.[5]

Claim 1

Claim 1 recites:

> A method comprising:
> sensing a user device coupled to a port of a network access device;
> determining if the user device supports a user authentication protocol; and

[4] M.P.E.P. §707.07(d).

[5] Manual of Patent Examining Procedure (MPEP) § 2131. See also *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

> placing the port into a semi-authorized access state if it is determined that the user device does not support the user authentication protocol, the semi-authorized access state providing the user device with limited network access.

The Examiner states:

> … Meier et al. clearly disclose and show a method comprising: sensing a user device (fig. 3 (302), paragraph 0032 (WSTA attempting to gain **access** to AP)) coupled to a port **of a** network access device (paragraph 0032 (attempting to gain access to AP));
> determining if said user device supports a user authentication protocol (paragraph 0032 (AP attempts to authenticate the WSTA)); and
> placing the port into a semi-authorized access state (paragraph 0022 (default guest set)) if it is determined that the user device does not support the user authentication protocol (paragraph 0022 (unauthorized guest WSTAs)), the semi-authorized access state providing the user device with limits access (paragraph 0022 (restricted access)).[6]

The Applicant respectfully disagrees for the reasons set forth below.

Meier et al. Does Not Disclose Determining If The User Device Supports A User Authentication Protocol

Contrary to the Examiner's statement, Meier et al. does not disclose determining if the user device supports a user authentication protocol as required be Claim 1. In support of the Examiner's statement, the Examiner refers to the following portion of Meier et al.:

> Referring now to FIG. 3 there is shown a WSTA 302 attempting to gain access to AP 102. A message is sent from WSTA 302 to the AP 102. The AP 102 then attempts to authenticate the WSTA 302 by sending authentication message 306 comprising the WSTA 302 and the WSTA's SSID to security server 304. If the security server 304 authenticates WSTA 302, it then sends a message 308 containing parameters for the WSTA 302 to the AP 102.[7]

The above portion of Meier et al. cited by the Examiner merely discloses determining whether a device is authenticated to an access point (AP). The cited portion of Meier et al. says nothing

[6] Office Action at pp. 2-3.
[7] Meier et al. at ¶ 32.

about a *user* authentication protocol, let alone determining whether a user device *supports* a particular user authentication protocol. The Applicant respectfully submits it is improper to equate determining whether a user device does supports a user authentication protocol, with determining whether the information exchanged in an authentication protocol *supported* by the user device is properly authenticated.

For at least the above reasons, the 35 U.S.C. § 102 Rejection of Claim 1 based on Meier et al. is unsupported by the cited art of record. Thus, a *prima facie* case has not been established and the rejection must be withdrawn.

Independent Claims 30 and 31

Claim 30 is an *In re Beauregard* claim corresponding to method claim 1. Claim 31 is a means-plus-function apparatus claim corresponding to method claim 1. Claim 1 being allowable, Claims 30 and 31 must also be allowable for at least the same reasons as for Claim 1.

Dependent Claims 2-10

Claims 2-10 depend from Claim 1. Claim 1 being allowable, Claims 2-10 must also be allowable for at least the same reasons as for Claim 1.

Independent Claims 32, 40, and 41

Contrary to the Examiner's statement, Meier et al. does not disclose allowing the user device limited access to a network via the network access device if it is determined that the user device is unable to communicate using a particular user authentication protocol as required by claims 32, 40, and 41. In support of the Examiner's statement, the Examiner refers to the rejection of Claim 1. However, the portion of Meier et al. cited by the Examiner merely discloses determining whether a device is authenticated to an access point (AP); the cited portion of Meier et al. says nothing about a *user* authentication protocol, let alone determining that the user device is *unable to communicate* using a particular user authentication protocol as required by Claims 32, 40, and 41.

Dependent Claims 33-35

Claims 33-35 depend from Claim 32. Claim 32 being allowable, Claims 33-35 must also be allowable for at least the same reasons as for Claim 32.

The 35 U.S.C. § 103 Rejection

Claims 11-19, 20-29, and 36-39 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Roese et al.[8] in view of Meier et al., among which claims 11, 20, and 36 are independent claims.[9] This rejection is respectfully traversed.

Claims 13-14 and 22-23 were previously cancelled without prejudice or disclaimer of the subject matter contained therein, rendering the rejection moot as to Claims 13-14 and 22-23.

[8] U.S. Publication No. 2003/0217151 to Roese et al.

[9] Office Action at p. 7.

Improper Omnibus Rejection

As an initial matter, the Applicant submits that the omnibus rejection of Claims 11-19, 20-29, and 36-39 under 35 U.S.C. § 103 is improper. The Examiner has grouped 3 independent claims into a single omnibus rejection under 35 U.S.C. § 103. The rejection refers to the term "control logic adapted to determine whether a user device coupled to one of the plurality of input ports supports a user authentication protocol used by a host network." Claims 11 and 20 refer to refer to "control logic adapted to determine whether a user device coupled to one of the plurality of input ports supports a user authentication protocol used by a host network," while Claim 36 refers to "control logic configured to allow the user device limited access to a network *if it is determined that the user device is unable to communicate using a particular user authentication protoco*l" (emphasis added) The omnibus rejection under 35 U.S.C. § 103 is therefore not equally applicable to all claims in the group and is thus improper.

Turning to the substance of the rejection, according to the Manual of Patent Examining Procedure (M.P.E.P.),

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure.[10]

Claim 11

Claim 11 recites:

A network access device comprising:
a plurality of input ports;

[10] M.P.E.P § 2143.

a plurality of output ports;
a switching fabric for routing data received on the plurality of input ports to at least one of the plurality of output ports; and
control logic adapted to determine whether a user device coupled to one of the plurality of input ports supports a user authentication protocol used by a host network, and to place the one of the input ports in a semi-authorized access state if the authentication protocol is not supported, the semi-authorized access state providing the user device with limited network access.

The Examiner states:

> ... Roese et al., clearly disclose and show a network access device comprising:
> a plurality of input ports (fig.8 (106a & i), paragraph 27);
> a plurality of output ports (fig.8 (106g & f), paragraph 27);
> a switching fabric (fig. 1(136 – switching device), paragraph 27) for routing data received on said plurality of input ports to at least one of said plurality of output ports; and
> control logic (paragraph 100 (802.1x to authenticate user for network access control)) adapted to determine whether a user device coupled to one of said plurality of input ports supports a user authentication protocol (paragraph 100 (802.1x to authenticate user for network access control)) used by a host network. However, Roese et al. do not specifically disclose placing the one input ports in a semi-authorized access state if the authentication protocol is not supported, the semi-authorized access state providing the user device with limited network access.
> In the same field of endeavor, Meier et al. clearly show placing the one of the input ports in a semi-authorized access state (paragraph 0022 (default guest set)) if the authentication protocol is not supported (paragraph 0022 (unauthorized guest WSTAs)), the semi-authorized access state providing the user device with limited network access ((paragraph 0022 (restricted access))
> Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method for providing multiple access modes, as taught by Roese, and show placing the one input ports in a semi-authorized access state if the authentication protocol is not supported, the semi-authorized access state providing the user device with limited network access,as taught by Meier, so that network access can be performed smoothly.[11]

The Applicant respectfully disagrees for the reasons outlined below.

Roese et al. in view of Meier et al. Does Not Disclose or Suggest Determining If The User Device Supports A User Authentication Protocol

Contrary to the Examiner's statement, Roese et al. in view of Meier et al. does not disclose or suggest control logic adapted to determine whether a user device coupled to one of

[11] Office Action at pp. 7-8.

the plurality of input ports supports a user authentication protocol used by a host network as required by Claim 11. The Applicant notes that in the Office Action mailed February 20, 2008, the Examiner admits that Roese et al. does not disclose or suggest this limitation.[12] Now the Examiner refers to the following portion of Roese et al. in support of the Examiner's contention:

> [0100] As described in the overview example, location information allows system 100 to authenticate and restrict a user based on the location of the device used by the user to access the network. The location information can be added as an authentication attribute to typical authentication systems. Entry into and usage of a network is typically regulated using authentication systems such as Network Operating Systems (NOSs), Remote Authentication Dial-In User Service (RADIUS), described in IETF Request For Comment (RFC) 2138, and IEEE 802.1X standard, which provides for port-based network access control based on a MAC identifier. In the case of NOS and RADIUS, an authentication server (e.g., 142 (FIG. 8)) provides the mechanism for establishing such authentication. In the case of IEEE 802.1X, the network entry devices 114 may be configured with such authentication capability, as described more fully in that standard. IEEE 802.1 Q standard provides another means for controlling access and usage of a network. That standard is directed to the establishment and operation of VLANs. The IEEE 802.1Q standard defines the configuration of network devices to permit packet reception at a configured port entry module. Firewalls (e.g., 140 (FIG. 8)) also provide a technique for network usage regulation.[13]

The above portion of Roese et al. cited by the Examiner provides a laundry list of authentication systems but says nothing about control logic adapted to determine whether a user device coupled to one of the plurality of input ports *supports* a user authentication protocol used by a host network as required by Claim 11. The Applicants respectfully submit the Examiner's attempt to equate identification information with the mechanism (authentication protocol) by which identification information is exchanged or communicated between entities, is improper.

For at least the above reasons, the 35 U.S.C. § 103 Rejection of Claim 11 based on Roese et al. in view of Meier et al. is unsupported by the cited art of record. Thus, a *prima facie* case has not been established and the rejection must be withdrawn.

[12] Office Action mailed February 20, 2008, p. 5. ll. 3-4.

[13] Roese et al. at ¶ 100.

Independent Claim 20

Claim 20 is a non-means-plus-function system claim corresponding to non-means-plus-function apparatus claim 11. Claim 11 being allowable, Claim 20 must also be allowable for at least the same reasons as Claim 11.

Dependent Claims 12-19, and 21-29

Claims 12-19 depend from Claim 11. Claims 21-29 depend from Claim 20. Claims 11 and 20 being allowable, Claims 12-19, and 21-29 must also be allowable for at least the same reasons as for Claims 11 and 20.

Independent Claim 36

Contrary to the Examiner's statement, Roese et al. in view of Meier et al. does not disclose control logic configured to allow the user device limited access to a network if it is determined that the user device is unable to communicate using a particular user authentication protocol. as required by claim 36. In support of the Examiner's statement, the Examiner refers to the rejection of Claim 11. However, the portion of Roese et al. cited by the Examiner provides a laundry list of authentication systems but says nothing about control logic configured to allow the user device limited access to a network if it is determined that the user device is unable to communicate using a particular user authentication protocol. as required by claim 36. For at least the above reasons, the 35 U.S.C. § 103 Rejection of Claim 36 based on Roese et al. in view of Meier et al. is unsupported by the cited art of record. Thus, a *prima facie* case has not been established and the rejection must be withdrawn.

Dependent Claims 37-39

Claims 37-39 depend from Claim 36. Claim 36 being allowable, Claims 37-39 must also be allowable for at least the same reasons as for Claim 36.

In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

Conclusion

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited.

If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

The Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Please charge any additional required fee or credit any overpayment not otherwise paid or credited to our deposit account No. 50-3557.

Respectfully submitted,

NIXON PEABODY LLP

Dated: February 4, 2009

/John P. Schaub/
John P. Schaub
Reg. No. 42,125

NIXON PEABODY LLP
200 Page Mill Road, 2nd Floor
Palo Alto, CA 94306
Tel. (650) 320-7700
Fax. (650) 320-7701